Journal of Combinatorial Theory, Series B **74**, 378–396 (1998)
Article No. TB981860

Bicycle Dimension and Special Points of the Tutte Polynomial

Dirk Vertigan

Department of Mathematics, Louisiana State University, Baton Rouge, Louisiana 70803
E-mail: vertigan@math.lsu.edu

Received January 6, 1998

For each pair of algebraic numbers (x, y) and each field F, the complexity of computing the Tutte polynomial $T(M; x, y)$ of a matroid M representable over F is determined. This computation is found to be $\overline{\#\mathrm{P}}$-complete except when $(x-1)(y-1)=1$ or when $|F|$ divides $(x-1)(y-1)$ and (x, y) is one of the seven points $(0, -1)$, $(-1, 0)$, $(i, -i)$, $(-i, i)$, (j, j^2), (j^2, j) or $(-1, -1)$, where $j=e^{2\pi i/3}$. Expressions are given for the Tutte polynomial in the exceptional cases. These expressions involve the bicycle dimension of M over F. A related result determines when this bicycle dimension is well defined.

Key Words: Tutte polynomial; matroids; computational complexity; polynomial time; $\#$P-complete.

1. INTRODUCTION

It was shown in [11] that, for fixed numbers x and y, computing the Tutte polynomial $T(G; x, y)$ of a graph G is $\overline{\#\mathrm{P}}$-complete, unless $(x-1)(y-1)=1$, or (x, y) is one of nine special points. In general, we wish to address the question, given a class of matroids $\mathscr{M}$ and fixed numbers (x, y), what is the complexity of computing $T(M; x, y)$ for $M \in \mathscr{M}$? Now, for any matroid, the Tutte polynomial is trivial to compute whenever $(x-1)(y-1)=1$. If the class $\mathscr{G}$ of graphic matroids is contained in $\mathscr{M}$, then this question can be resolved by settling it for the special points. The purpose of this paper is to resolve this question for the seven special points other than the point $(1, 1)$, which is dealt with in another paper [17], and the point $(0, 0)$, which is trivial. The polynomial time computability results and the $\overline{\#\mathrm{P}}$-completeness results are obtained by somewhat different, but not totally unrelated, means. In the former case one can relate the value of the Tutte polynomial to the dimension of the bicycle space of a represented matroid, that is, the intersection of the cycle and cocycle spaces of the representation.

0095-8956/98 $25.00

Most of the results are obtained by examining ratios between the *pointed* Tutte polynomials of a matroid. Pointed Tutte polynomials first appear in [3]. The main theorems are stated in Section 3, while the proofs are completed in Section 7. Most of the work towards the proofs appears in Sections 5 and 6. These sections are based on ideas from [11] and [10], respectively. Also in Section 3 is a matroid-theoretic result about when bicycle dimension is well-defined, which, while of a different nature, relates closely to the other results.

Further results are presented in Section 8.

2. PRELIMINARIES

For matroid theory terminology and notation, we follow Oxley [12]. The Tutte polynomial is a two-variable polynomial invariant defined originally for graphs [15], [20], but later extended to matroids [2], [5]. The *Tutte polynomial* of a matroid $M=(S, \rho)$, with ground set S and rank function ρ, is defined to be

$$T(M; x, y)=\sum_{A \subseteq S}(x-1)^{\rho(S)-\rho(A)}(y-1)^{|A|-\rho(A)}. \tag{1}$$

Let $\mathscr{G}$, respectively, $\mathscr{PG}$, denote the class of cycle matroids of graphs, respectively, planar graphs. For a field F, let $\mathscr{M}_F$ denote the class of matroids representable over F. (If F is finite, we also denote $\mathscr{M}_F$ by $\mathscr{M}_{|F|}$.) Let S be a finite set. The set F^S of all functions $v: S \to F$ can be made into a vector space over F in the obvious way. For $v \in F^S$ define the *support* of v, $\mathrm{supp}(v)$, to be $\{s \in S \mid v(s) \neq 0\}$ and the *weight*, $w(v)$, of v to be $|\mathrm{supp}(v)|$. For $u, v \in F^S$ define $\langle u, v\rangle = \sum_{s \in S} u(s)\, v(s)$. Consider a subspace V of F^S and call V an *F-space on S*. The *dual space* V^*, of V, is defined to be $\{u \mid u \in F^S, \langle u, v\rangle = 0 \text{ for all } v \in V\}$. Let $M(V)$ denote the matroid, with ground set S, whose circuits are the minimal non-empty supports of vectors in V. Equivalently, $M(V)$ is represented by any matrix whose rows span V^*. When $F=\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ an F-space V and matroid $M(V)$ are called, respectively, *binary*, *ternary* and *quaternary*. Often, in notation, $\mathbb{F}_q$ is replaced by q or is omitted.

For terminology and notation in computational complexity, we follow Welsh [19]. Every complexity class we consider will be a class of *functions* $f: \{0, 1\}^* \to \{0, 1\}^*$ where $\{0, 1\}^*$ is the set of binary strings. We assume that the objects we consider, such as graphs, matrices, rationals, polynomials, etc., are all encoded as binary strings in a standard way. We let $f \leqslant_T g$ denote that the function f is polynomial time Turing reducible to g.

For a class of functions $\mathscr{F}$, we let $\mathrm{FP}^{\mathscr{F}}$ denote $\{f \mid f \leqslant_T g \text{ for some } g \in \mathscr{F}\}$. Also g is *$\mathscr{F}$-complete* if $g \in \mathscr{F}$ and $\mathrm{FP}^{\mathscr{F}} = \mathrm{FP}^{\{g\}}$.

The two main classes we consider are FP, the class of polynomial time computable *functions* and $\#\mathrm{P}$, a well-known class of counting problems introduced in [16]. Actually, since most evaluations of the Tutte polynomial are not literally counting problems, we often use the class $\mathrm{FP}^{\#\mathrm{P}}$, the class of functions polynomial time Turing reducible to a function in $\#\mathrm{P}$. We abbreviate $\mathrm{FP}^{\#\mathrm{P}}$ to $\overline{\#\mathrm{P}}$. All the functions considered in this paper are either shown to be $\overline{\#\mathrm{P}}$-complete or to be in FP.

Let $\mathscr{C}$ be a class of matroids and e: $\{0, 1\}^* \to \mathscr{C}$ an encoding of matroids as binary strings. Note that many strings may encode the same matroid.

1. DEFINITION. The class of matroids $\mathscr{C}$ (together with encodinq e) is *rank-succinct* if there is a polynomial p such that for every matroid $M = (S, \rho) \in \mathscr{C}$ and every string w with $e(w) = M$:

(i) $|S| \leqslant |w| \leqslant p(|S|)$, and

(ii) for every $A \subseteq S$, $\rho(A)$ can be computed in time $p(|S|)$.

This technical condition is satisfied by all the classes of matroids we consider, unless otherwise stated. All of the functions we consider will take, as input, a matroid $M \in \mathscr{C}$ and will output its Tutte polynomial $T(M; x, y)$ or some specialization thereof. The technical details of how to represent the outputs are considered in [18].

Define the function

$$\tau^2(\mathscr{C}) : \mathscr{C} \to \mathbb{Z}[x, y] \qquad \text{where} \quad M \mapsto T(M; x, y).$$

This function determines the Tutte polynomial of each matroid $M \in \mathscr{C}$ on the whole (x, y)-plane.

Let $\mathbb{A}$ denote the set of algebraic numbers. For any fixed algebraic point $(x_0, y_0) \in \mathbb{A}^2$, define the function

$$\tau^0(\mathscr{C}, x_0, y_0) : \mathscr{C} \to \mathbb{Q}(x_0, y_0) \qquad \text{where} \quad M \mapsto T(M; x_0, y_0).$$

This function determines the Tutte polynomial of each matroid $M \in \mathscr{C}$ at a single point (x_0, y_0).

For an algebraic curve, the function $\tau^1(\mathscr{C}, K)$ sends matroid $M \in \mathscr{C}$ to the Tutte polynomial of M "along" the curve K (as defined in [18]).

The functions $\tau^2(\mathscr{C})$, $\tau^1(\mathscr{C}, K)$, and $\tau^0(\mathscr{C}, x_0, y_0)$ are called *Tutte invariants*. As shown in [18], all these Tutte invariants are in $\overline{\#\mathrm{P}}$, provided $\mathscr{C}$ is rank-succinct.

The following lemma makes some trivial observations which simplify the case analysis.

2.1. LEMMA. *If (x_0, y_0) is an algebraic point and K is an algebraic curve containing (x_0, y_0), then*

$$\tau^0(\mathscr{C}, x_0, y_0) \leqslant_T \tau^1(\mathscr{C}, K) \leqslant_T \tau^2(\mathscr{C}). \tag{2}$$

If $\mathscr{C}' \subseteq \mathscr{C}$ are classes of matroids, and $\mathscr{C}'$ (but not necessarily $\mathscr{C}$) is rank-succinct, and from every encoding of every $M \in \mathscr{C}'$ an encoding of $M \in \mathscr{C}$ can be found in polynomial time, then

$$\tau^0(\mathscr{C}', x_0, y_0) \leqslant_T \tau^0(\mathscr{C}, x_0, y_0),\ \tau^1(\mathscr{C}', K) \leqslant_T \tau^1(\mathscr{C}, K),\ \tau^2(\mathscr{C}') \leqslant_T \tau^2(\mathscr{C}). \tag{3}$$

For a matroid $M = (S, \rho)$,

$$\text{if} \quad (x, y) \in H_1, \qquad \text{then} \quad T(M; x, y) = (x-1)^{\rho(S)} (y-1)^{|S|}. \tag{4}$$

Moreover, if for every matroid $M = (S, p) \in \mathscr{C}$, the size $|S|$ and rank $p(S)$ of M can be found in polynomial time (in particular if $\mathscr{C}$ is rank-succinct), then

$$\tau^1(\mathscr{C}', H_1) \qquad \text{is in FP.} \tag{5}$$

We define certain curves and points wich play a special role in the results of this paper. For each $q \in \mathbb{A}$, define the curve $H_q = \langle (x, y) \mid (x-1)(y-1) = q \rangle$ and define $H_0^x = \langle (x, y) \mid x = 1 \rangle$ and $H_0^y = \langle (x, y) \mid y = 1 \rangle$. The curves H_0^x, H_0^y, and H_q for $q \in \mathbb{A} - \{0\}$ are called *special curves*. Let $j = e^{2\pi i/3}$. The points $(1, 1)$, $(0, 0)$, $(-1, -1)$, $(0, -1)$, $(-1, 0)$, $(i, -i)$, $(-i, i)$, (j, j^2), (j^2, j) are called *special points*. Observe that these points are on H_q where, respectively, $q = 0, 1, 4, 2, 2, 2, 2, 3, 3$. A *movable special point* is a special point other than $(0, 0)$ or $(1, 1)$.

The following is Proposition 1 of [11].

2.2. PROPOSITION. (i) *The function $\tau^2(\mathscr{G})$ is $\overline{\#\mathrm{P}}$-complete.*

(ii) *If K is an algebraic curve then $\tau^1(\mathscr{G}, K)$ is $\overline{\#\mathrm{P}}$-complete unless $K = H_1$ in which case $\tau^1(\mathscr{G}.K)$ is in* FP.

(iii) *If $(x, y) \in \mathbb{A}^2$ is an algebraic point then $\tau^0(\mathscr{G}, x, y)$ is $\overline{\#\mathrm{P}}$-complete unless $(x, y) \in H_1$ or (x, y) is a special point, in which case $\tau^0(\mathscr{G}, x, y)$ is in* FP.

3. THE MAIN RESULT

The main computational complexity result, proved in Section 7, using lemmas from earlier sections, is the following.

3.1. THEOREM. *For any finite field F:*

(i) *The function $\tau^2(\mathcal{M}_F)$ is $\overline{\#\mathrm{P}}$-complete.*

(ii) *If K is an algebraic curve, then $\tau^1(\mathcal{M}_F, K)$ is $\overline{\#\mathrm{P}}$-complete unless K is H_1, in which case $\tau^1(\mathcal{M}_F, K)$ is in* FP.

(iii) *If $(x, y) \in \mathbb{A}^2$ then $\tau^0(\mathcal{M}_F, x, y)$ is $\overline{\#\mathrm{P}}$-complete unless $(x, y) \in H_1$ or (x, y) is a movable special point on H_q with $|F|$ dividing q, in which case, $\tau^0(\mathcal{M}_F, x, y)$ is in* FP.

We deal with infinite fields in Theorem 8.5, Section 8. Note that by Proposition 2.2 and Lemma 2.1 we need only consider computations at special points.

The following lemma, which is readily verified, could be used to rephrase part (iii) of the above theorem statement more explicitly.

3.2. LEMMA. *(x, y) is a movable special point on H_q with $|F|$ dividing q if and only if*

(i) *$|F| = 2$ and (x, y) is one of $(-1, -1)$, $(0, -1)$, $(-1, 0)$, $(i, -i)$, $(-i, i)$; or*

(ii) *$|F| = 3$ and (x, y) is one of (j, j^2), (j^2, j); or*

(iii) *$|F| = 4$ and (x, y) is $(-1, -1)$.*

Let $\mathcal{M}_{\mathrm{reg}} = \mathcal{M}_2 \cap \mathcal{M}_3$ be the class of *regular matroids*, namely matroids representable over every field.

3.3. COROLLARY. (i) *The function $\tau^2(\mathcal{M}_{\mathrm{reg}})$ is $\overline{\#\mathrm{P}}$-complete.*

(ii) *If K is an algebraic curve, then $\tau^1(\mathcal{M}_{\mathrm{reg}}, K)$ is $\overline{\#\mathrm{P}}$-complete unless $K = H_1$, in which case, $\tau^1(\mathcal{M}_{\mathrm{reg}}, K)$ is in* FP.

(iii) *If $(x, y) \in \mathbb{A}^2$ is an algebraic point then $\tau^0(\mathcal{M}_{\mathrm{reg}}, x, y)$ is $\overline{\#\mathrm{P}}$-complete unless $(x, y) \in H_1$ or (x, y) is a special point, in which case, $\tau^0(\mathcal{M}_{\mathrm{reg}}, x, y)$ is in* FP.

Proof. Since $\mathcal{G} \subseteq \mathcal{M}_{\mathrm{reg}} \subseteq \mathcal{M}_F$ for every (finite) field F, the result follows from Proposition 2.2 and Theorem 3.1, except for the case $(x, y) = (1, 1)$. Since $T(M; 1, 1)$ counts the number of bases of a matroid, this can be determined in polynomial time for regular matroids using Kirchoff s determinantal formula. ∎

The proof of Theorem 3.1 also gives rise to the theorem below. Let F be a field and let α be an automorphism of F. Let S be a finite set. For a

vector $v \in F^S$ or subspace $V \subseteq F^S$, abuse notation and define $\alpha(v)$ and $\alpha(V)$ in the natural way. Define

$$d(V, F, \alpha) = \dim(V \cap \alpha(V^*)).$$

When $|F| = q \in \{2, 3, 4\}$ and $\alpha(x) = x^{-1}$ for $x \in F - \{0\}$, abbreviate this to $d(V, q)$. (Note that, in this case, α is the identity for $q = 2, 3$, but not for $q = 4$.) When F and α are known, abbreviate further to $d(V)$. In the theorem below, whose proof is completed in Section 7, the case (j^2, j) with $|F| = 3$ was proved in [10] and the case $(-1, -1)$ with $|F| = 2$ (but not with $|F| = 4$) has been noted by various authors.

3.4. THEOREM. *For every binary space V,*

$$|T(M(V); -i, i)| = \begin{cases} \sqrt{2}^{d(V, 2)} & \text{if } 4 \mid w(v) \text{ for all } v \in V \cap V^* \\ 0 & \text{otherwise.} \end{cases} \tag{6}$$

For every ternary space V,

$$|T(M(V); j^2, j)| = \sqrt{3}^{d(V, 3)}. \tag{7}$$

For every quaternary space V,

$$T(M(V); -1, -1) = (-1)^{|S|}(-2)^{d(V, 4)}. \tag{8}$$

Observe that, for $q = 2, 3, 4$, the number $d(V, q)$ depends only on $M(V)$. In this case, $d(V, q)$ is called the *bicycle dimension (over $\mathbb{F}_q$)* of $M(V)$ and is also denoted $d(M(V), q)$. Note that if M is binary then it is also quaternary and $d(M, 2) = d(M, 4)$. However if M is both ternary and quaternary, then $d(M, 3)$ and $d(M, 4)$ need not be equal.

The result below is another by-product of the examination of complexity questions. One may ask in general when $d(V, F, \alpha)$ depends only on $M(V)$. For certain pairs (F, α), the bicycle dimension $d(V, F, \alpha)$ will be zero for every finite set S and every F-space V on S. This will hold if $\langle v, \alpha(v) \rangle \neq 0$ for every vector $v \neq 0$, in which case, F must have characteristic zero. (This occurs, for example, when F is the rationals, and α is the identity, or when F is the complex numbers and α is complex conjugation.) But otherwise there are only three cases of the above kind of invariance as stated below.

3.5. PROPOSITION. *Let F be a field and let α be an automorphism of F. Suppose there exists a finite set S and a vector $v \in F^S - \{0\}$ such that $\langle v, \alpha(v) \rangle = 0$. Then* (i) *and* (ii) *are equivalent.*

(i) *For every finite set S and all F-spaces U, V on S, if $M(U) = M(V)$, then $d(U) = d(V)$.*

(ii) *The field F is $\mathbb{F}_2$, $\mathbb{F}_3$ or $\mathbb{F}_4$ and automorphism $\alpha: F \to F$ is such that $\alpha(x) = x^{-1}$ for $x \neq 0$.*

Proof. Suppose (i) holds. Let the finite set S and vector $v \in F^S - \{0\}$ be such that $\langle v, \alpha(v) \rangle = 0$. Without loss of generality, we can assume that $\mathrm{supp}(v) = S$. Let $V = \mathrm{span}(v)$, the one-dimensional subspace of F^S generated by v. Then $v \in V \cap \alpha(V^*)$ and $d(V) = 1$.

Let $n = |S|$. Let $u \in F^S$ with $\mathrm{supp}(u) = S$ and let $U = \mathrm{span}(u)$. Then it is easily seen that $M(U) = M(V) \cong U_{n-1,n}$. Thus $d(U) = 1$, by (i). It follows that $\sum_{s \in S} u(s)\, \alpha(u(s)) = 0$ for every $u \in F^S$ with $\mathrm{supp}(u) = S$. This is only possible if, for every $a \in F - \{0\}$, we have $a\alpha(a) = 1\alpha(1) = 1$, and hence $\alpha(a) = a^{-1}$. In particular, for $a \in F - \{0, -1\}$, we have $a^{-1} + 1^{-1} = (a+1)^{-1}$ so that $a^2 + a + 1 = 0$ and hence $F \subseteq \{0, -1\} \cup \{a \mid a \in F,\ a^2 + a + 1 = 0\}$. Therefore $|F| \leqslant 2 + 2 = 4$, and (ii) follows.

Conversely suppose that (ii) holds. It is already known that (i) follows for $q = 2, 3$. Also for $q = 2, 3, 4$, (i) follows easily from Theorem 3.4. ∎

4. FURTHER PRELIMINARIES

We now present more background material needed for the proofs of the results.

A *pointed* matroid (M, s) is simply a matroid $M = (S, \rho)$ together with an element $s \in S$. Define

$$\begin{aligned} C(M, s) &= \{A \mid s \in A \subseteq S,\ \rho(A) = \rho(A - \{s\}) + 1\} \\ L(M, s) &= \{A \mid A \subseteq S - \{s\},\ \rho(A \cup \{s\}) = \rho(A)\}. \end{aligned} \tag{9}$$

The *pointed* Tutte polynomials are defined by

$$T_C(M, s; x, y) = \sum_{A \in C(M, s)} (x-1)^{\rho(S) - \rho(A)}\, (y-1)^{|A| - \rho(A)} \tag{10}$$

$$T_L(M, s; x, y) = \sum_{A \in L(M, s)} (x-1)^{\rho(S) - \rho(A)}\, (y-1)^{|A| - \rho(A)}. \tag{11}$$

When x, y, M, s are known from the context, abbreviate $T(M; x, y)$, $T(M \backslash s; x, y)$, $T(M/s; x, y)$, $T_C(M, s; x, y)$ and $T_L(M, s; x, y)$ to T, T', T'', T_C and T_L, respectively. It can be shown that if s is not a loop or coloop, then

$$\begin{aligned} T &= T' + T'' \\ T &= xT_C + yT_L \\ T' &= (x-1)\,T_C + T_L \\ T'' &= T_C + (y-1)\,T_L. \end{aligned} \tag{12}$$

If s is a coloop, then

$$T = xT'', \qquad T' = T'' = T_C, \qquad T_L = 0. \tag{13}$$

If s is a loop, then

$$T = yT', \qquad T' = T'' = T_L, \qquad T_C = 0. \tag{14}$$

In all cases, any two of T, T', T'', T_C, or T_L, determine the others, provided $(x-1)(y-1) \neq 1$. Also $A \in L(M, s)$ if and only if $S - A \in C(M^*, s)$. It follows that

$$\begin{aligned} &T_C(M^*, s; x, y) = T_L(M, s; y, x) \qquad \text{and} \\ &T_L(M^*, s; x, y) = T_C(M, s; y, x). \end{aligned} \tag{15}$$

Brylawski [3] defines the 2-*sum* of two pointed matroids, see also [12]. The *tensor product* [3] $N \otimes_s M$ of a matroid $N = (E, \mu)$ and a pointed matroid (M, s), with $M = (S, \rho)$ and $s \in S$, is obtained by 2-summing of (M, s) to every point of N. (If s is clear frorn the context, we omit it from the notation.) It is shown in [3] that, provided $T_C \neq 0$ and $T_L \neq 0$,

$$\begin{aligned} &T(N \otimes_s M; x, y) = T_C^{|E| - \mu(E)}\, T_L^{\mu(E)}\, T(N; X, Y) \\ &\text{where} \quad (X, Y) = \left(1 + (x-1)\frac{T_C}{T_L},\, 1 + (y-1)\frac{T_L}{T_C}\right) = \left(\frac{T'}{T_L}, \frac{T''}{T_C}\right). \end{aligned} \tag{16}$$

The *k-thickening* (respectively, *k-stretch*) of a matroid N is $N \otimes U_{1,k+1}$ (respectively, $N \otimes U_{k,k+1}$) is obtained by replacing each point of N with k points in parallel (respectively, in series). We place another technical condition on all the classes of matroids we consider (unless otherwise stated).

2. Definition. The class of matroids $\mathscr{C}$ (together with encoding e: $\{0, 1\}^* \to \mathscr{C}$) is *expand-succinct* if:

(i) $\mathscr{C}$ (together with encoding e) is *rank-succinct*, and

(ii) for every integer $k \geqslant 3$, the class of matroids $\mathscr{C}$ is closed under k-stretches and k-thickenings and these can be constucted in time polynomial in k and the size of the matroid.

Recall that if (x_0, y_0) is an algebraic point and K is an algebraic curve containing (x_0, y_0), then trivially,

$$\tau^0(\mathscr{C}, x_0, y_0) \leqslant_T \tau^1(\mathscr{C}, K) \leqslant_T \tau^2(\mathscr{C}). \tag{17}$$

It was shown in [11] that in certain cases, stated below, these reducibilities can be reversed. The results of [11] make much use of Equation (16), as do the results of this paper. The following is Theorem 1 of [11]. (It was only proved for rational curves but it is straightforward to extend this to algebraic curves, although this extension is not used here.)

4.1. THEOREM. *Let $\mathscr{C}$ be an expand-succinct class of matroids. If K is an algebraic curve, then $\tau^2(\mathscr{C}) \leqslant_T \tau^1(\mathscr{C}, K)$ unless K is a special curve.*

The following is Theorem 2 of [11].

4.2. THEOREM. *Let $\mathscr{C}$ be an expand-succinct class of matroids. If K is a special curve and $(x, y) \in K$, then $\tau^1(\mathscr{C}, K) \leqslant_T \tau^0(\mathscr{C}, x, y)$ unless (x, y) is a special point.*

5. SPOILERS

In this section, we prove the following lemma, which plays a major role in the proof of Theorem 3.1.

5.1. LEMMA. *If (x, y) is a movable special point and $|F|$ does not divide $(x-1)(y-1)$, then $\tau^0(\mathscr{M}_F, x, y)$ is $\overline{\#\mathrm{P}}$-complete.*

Let $M = (S, \rho)$ be a matroid and $s \in S$. Let (x, y) be a movable special point. (Many arguments here apply to any $(x, y) \in \mathbb{A}^2$, but this is not needed.) Let T, T', T'', T_C, T_L be as in Section 4. If $T_C, T_L \neq 0$, then let

$$(X, Y) = \left(1 + (x-1)\frac{T_C}{T_L}, 1 + (y-1)\frac{T_L}{T_C}\right) = \left(\frac{T'}{T_L}, \frac{T''}{T_C}\right). \tag{18}$$

Let H_q be the special curve containing (x, y), and hence (X, Y), so that $q = (x-1)(y-1) = (X-1)(Y-1)$. The pointed matroid (M, s) *spoils* (x, y) if $T_C, T_L \neq 0$ and (X, Y) is not a special point. We also say M spoils (x, y) if (M, s) spoils (x, y) for some s. This section is based on the following simple lemma.

5.2. LEMMA. *Let (M, s) be a fixed pointed matroid. Let $\mathscr{C}$ be an expand-succinct class of matroids such that if $N \in \mathscr{C}$ then $N \otimes_s M$ is in $\mathscr{C}$ and*

can be constructed in polynomial time. Let (x, y) *and* (X, Y) *be as above and let* K *be the special curve containinq* (x, y) *and hence* (X, Y). *Then*

$$\tau^0(\mathscr{C}, X, Y) \leqslant_T \tau^0(\mathscr{C}, x, y). \tag{19}$$

Furthermore, if (M, s) *spoils* (x, y), *then*

$$\tau^1(\mathscr{C}, K) \leqslant_T \tau^0(\mathscr{C}, x, y). \tag{20}$$

Proof. Recall Equation (16) in Section 4. The reduction for (19) is as follows. For input $N \in \mathscr{C}$, construct $N \otimes_s M$, apply oracle $\tau^0(\mathscr{C}, x, y)$ and divide by $T_C^{|E|-\mu(E)} T_L^{\mu(E)}$ to obtain $T(N; X, Y)$, as required. The rest follows immediately from Theorem 4.2. ▮

First note that if $(x, y) = (0, 0)$ or $(1, 1)$, then $(x, y) = (X, Y)$, regardless of (M, s), and the above lemma reveals nothing. Thus the question of the computational complexity of $\tau^0(\mathscr{M}_F, 1, 1)$ cannot be resolved by these methods and some other approach is required—see [17].

To prove Lemma 5.1, the idea is to combine Proposition 2.2 and Lemma 5.2 after finding spoilers for the movable special points. Pairs (M, s) which spoil (x, y) are essentially found by trial and error, but guessing to look at excluded minors of $\mathscr{M}_q$, $q = 2, 3, 4$, gives rapid results.

The matroids in the lemma below are all defined in [12]. Note that the matroid R_6 is the 2-sum of two $U_{2,4}$'s. The following lemma is routinely verified.

5.3. Lemma. (1a) $U_{2,4}$ *spoils* $(i, -i)$ *and* $(-i, i)$.

(1b) $U_{2,4}$ *is in* $\mathscr{M}_F$ *if and only if* $|F| > 2$.

(2a) R_6 *spoils* $(0, -1)$ *and* $(-1, 0)$.

(2b) R_6 *is in* $\mathscr{M}_F$ *if and only if* $|F| > 2$.

(3a) F_7 *and* F_7^* *spoil* (j, j^2) *and* (j^2, j).

(3b) F_7 *and* F_7^* *are in* $\mathscr{M}_F$ *if and only if* F *has characteristic* 2.

(4a) $U_{2,5}$ *and* $U_{3,5}$ *spoil* (j, j^2) *and* (j^2, j).

(4b) $U_{2,5}$ *and* $U_{3,5}$ *are in* $\mathscr{M}_F$ *if and only if* $|F| > 3$.

(5a) (F_7^-, s) *and* $((F_7^-)^*, s)$ *spoil* $(-1, -1)$ *for any element* s.

(5b) F_7^- *and* $(F_7^-)^*$ *are in* $\mathscr{M}_F$ *if and only if* F *has characteristic not* 2.

(6a) $U_{2,6}$, $U_{4,6}$, *and* P_6 *spoil* $(-1, -1)$.

(6b) $U_{2,6}$, $U_{4,6}$, *and* P_6 *are in* $\mathscr{M}_F$ *if and only if* $|F| > 4$.

Proof of Lemma 5.1. Since $\mathscr{G} \subseteq \mathscr{M}_F$ for every field F, the lemma follows from Proposition 2.2, Lemma 5.2 and Lemma 5.3. ▮

6. BICYCLE DIMENSION AND POLYNOMIAL TIME COMPUTABILITY

This section proves the following lemma, which essentially completes the proof of Theorem 3.1.

6.1. LEMMA. *If* (x, y) *is a movable special point and* $|F|$ *divides* $(x-1)(y-1)$, *then* $\tau^0(\mathscr{M}_F, x, y)$ *is in* FP.

The cases of Theorem 3.4 and Lemma 6.1 when $q=3$ are proved in [10], and the other cases are proved by essentially the same methods. The proof is preceded by some discussion and some other lemmas. Until further notice, we restict attention to the three cases, $(q, x, y)=(2, -i, i)$, $(3, j^2, j)$ and $(4, -1, -1)$, where $|F|=q$ and the automorphism α of F is such that $\alpha(x)=x^{-1}$ for $x\neq 0$.

The motivating idea for the proofs is as follows. If Lemma 6.1 and the well-known conjecture that $\mathrm{FP}\neq\overline{\#\mathrm{P}}$ are to hold, then by Lemma 5.2, it must be that no $M\in\mathscr{M}_q$ spoils (x, y). (Of course we claim no evidence for the $\mathrm{FP}\neq\overline{\#\mathrm{P}}$ conjecture.) Since, as noted in Section 4, any two of T, T', T'', T_C, T_L, determine the others, it would follow that there are only finitely many possibilities for (T, T', T'', T_C, T_L) up to a non-zero factor. In fact, it is routine to check that for $(q, x, y)=(4, -1, -1)$, $(3, j^2, j)$, $(2, -i, i)$, all the possibilities for (T, T', T'', T_C, T_L) up to a non-zero factor appear in Tables 1–3, respectively. (The other parts of the tables are explained throughout the section.) In the rightmost column of each table, we give names to various cases. It will be shown that for any (M, s) exactly one case holds, that it can be determined in polynomial time which case holds, and that the contents of each row are correct. Then the polynomial time algorithm for determining $T(M, x, y)$ with $M=(S, \rho)\in\mathscr{M}_q$, and with q, x, y as above, is as follows. Choose $s\in S$, determine which case applies to (M, s) and hence find the ratio $T: T'$ or $T: T''$. (If T' and T'' are both zero, then so is T and the answer is already found.) Repeat the process with T' (or T'' if $T'=0$) and proceed inductively until after $|S|$ such steps, the empty matroid (whose Tutte polynomial is 1) is reached. Multiplying the $|S|$ ratios gives T, computed in polynomial time, as required.

For an F-space V on S and $s\in S$, we now define the deletion and contraction of s from V. For $v\in F^S$, that is, $v\colon S\to F$, let $v-s$ denote $v\,|\,(S-\{s\})$. Define the *deletion* of s from V, denoted $V\backslash s$, to be $\{v-s\,|\,v\in V, v(s)=0\}$. Define the *contraction* of s from V, denoted V/s, to be $\{v-s\,|\,v\in V\}$. Observe that $V\backslash s$ and V/s are F-spaces on $S-\{s\}$. It is easy to check that, just as for matroids, $(V^*)^*=V$, $(V\backslash s)^*=(V^*)/s$, and $(V/s)^*=(V^*)\backslash s$. Also $M(V\backslash s)=(M(V))\backslash s$, $M(V/s)=(M(V))/s$, and $M(V^*)=(M(V))^*$.

The proof of Lemma 6.1 will use four subsidiary lemmas. Let F be a finite field and α an automorphism of F such that $\alpha \circ \alpha$ is the identity (as for the three cases in Theorem 3.4). Let S be a finite set, $s \in S$, and let V be an F-space on S. Let $1_s \in F^S$ satisfy $1_s(s) = 1$ and $1_s(t) = 0$ for $t \in S - \{s\}$.

6.2. LEMMA. *Exactly one of* (A), (Ba) $(a \in F)$ *holds.*

(A) *There exists* $v \in V \cap \alpha(V^*)$ *with* $v(s) \neq 0$.

(Ba) *There exists* $v \in V$ *and* $u \in \alpha(V^*)$ *with* $1_s = v + u$ *and* $v(s) = a$, $u(s) = 1 - a$. *Moreover, representinq* V *by a basis of* V *it can be determined in polynomial time, which case holds.*

Proof. Let (B) be the property $1_s \in V + \alpha(V^*)$. Now $\alpha(V + \alpha(V^*))^* = \alpha(V^*) \cap V$ so that (B) holds if and only if $\langle 1_s, \alpha(v) \rangle = 0$ for every $v \in V \cap \alpha(V^*)$. Clearly, (B) is the negation of (A). Also (B) holds exactly when (Ba) holds for some $a \in F$. Suppose $1_s = v + u = v' + u'$ where $v, v' \in V$ and $u, u' \in \alpha(V^*)$. Then $v - v' = u' - u$ is an element of $V \cap \alpha(V^*)$ and, since (A) does not hold, $v(s) = v'(s)$ and $u(s) = u'(s)$. Thus if (B) holds, then there is a unique $a \in F$ such that (Ba) holds.

Determining which case holds involves simple linear algebra algorithms. Given a basis for V, find a basis for $\alpha(V^*)$, for $V + \alpha(V^*)$ and for $V \cap \alpha(V^*)$. Now (A) holds if and only if $V \cap \alpha(V^*)$ has a basis element which is non-zero at s. Otherwise $1_s \in V + \alpha(V^*)$ and 1_s, is easily expressed as a linear combination of elements of V and $\alpha(V^*)$ and so $v \in V$ and $u \in \alpha(v^*)$ with $1_s = v + u$ are easily found, determining the unique $a = v(s)$ for which (Ba) holds. ∎

The element $s \in S$ is *of type* (A) *or* (Ba) $(a \in F)$, if s satisfies the corresponding property in the above lemma. Say s is a *loop* (respectively, *coloop*) of V if it is a loop (respectively, coloop) of $M(V)$ (or, equivalently, $1_s \in V$ (respectively, $v(s) = 0$ for all $v \in V$)). Observe that a loop is of type (B1) and a coloop is of type (B0). Abbreviate $d(V)$, $d(V \backslash s)$, $d(V/s)$ to d, d', d'', respectively.

6.3. LEMMA. *If* s *is a loop or coloop, then* $d = d' = d''$. *Otherwise*:

If s *is of type* (A), *then* $d = d' + 1 = d'' + 1$.
If s *is of type* $(B1)$, *then* $d = d' = d'' - 1$.
If s *is of type* $(B0)$, *then* $d = d' - 1 = d''$.
If s *is of type* (Ba) *where* $a \in F - \{0, 1\}$, *then* $d = d' = d''$.

Proof. This is proved for $F = \mathbb{F}_3$ in Proposition 2 of [10]. The proof makes no reference to the particular field used, and the automorphism α is easily incorporated to give a proof of this lemma. ∎

Let $\mathbb{F}_q$ be a finite field. Recall the weight $w(v)$ of a vector v from Section 2. If S is a finite set and V is an $\mathbb{F}_q$-space on S, then the *weight enumerator* of V is the one-variable polynomial

$$f(V; z) = \sum_{v \in V} z^{w(v)}. \tag{21}$$

If $M(V) = (S, \rho)$, then by [9],

$$f(V; z) = z^{\rho(S)}(1-z)^{|S|-\rho(S)}\, T\left(M(V); \frac{1}{z}, \frac{1+(q-1)z}{1-z}\right). \tag{22}$$

Tables I–III consider the points $(x, y) = (-1, -1)$, (j^2, j), and $(-i, i)$, respectively, and these correspond to $(q, z) = (4, -1)$, $(3, j)$, and $(2, i)$, respectively. From now on, assume that (q, z) takes one of these values. Given $s \in S$, abbreviate $f(V; z)$, $f(V\backslash s; z)$, $f(V/s; z)$ to f, f', f'', respectively. By Equation (22), (f, f', f'') is a non-zero scalar multiple of $(T, T'/(1-z), T''/z)$ if s is not a loop or coloop, of $(T, T'/(1-z), T''/(1-z))$ if s is a loop, or of $(T, T'/z, T''/z)$ if s is a coloop. The tables give (f, f', f'') and (T, T', T'', T_C, T_L) up to a non-zero factor in the various cases. By Equations (12)–(14) and (22), the ratio between any two of T, T', T'', T_C, T_L or between any two of f, f', f'' determines all other such ratios as well as (X, Y). It is routine to check that all the rows are consistent. It remains to define the various cases, to prove that these cases partition the set of possibilities, and that the contents of the row are correct whenever any given case holds.

The lemma below helps determine f/f' in certain cases. Let V be an $\mathbb{F}_q$-space on S, let $s \in S$ and suppose s is not a coloop, so that there exists $v \in V$ with $v(s) \neq 0$. Let $V' = \{v \mid v \in V, v(s) = 0\}$. Clearly $\dim(V) - 1 = \dim(V') = \dim(V\backslash s)$ and the map from $V' \subseteq F^S$ to $(V\backslash s) \subseteq F^{S-\{s\}}$ sending v to $v - s$ is a bijection which preserves weight. Thus $f' = f(V\backslash s; z) = f(V'; z)$. Also if $u \in V - V'$, then $V = V' + (u)$. Define $\hat{f} = \sum_{v \in V'} z^{w(v+u)}$. It is

TABLE I

$(q, x, y) = (4, -1, -1)$

T	T'	T''	T_C	T_L	f	f'	f''	$d-d'$	$d-d''$	X	Y	Case
1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{-1}{2}$	$\frac{-1}{2}$	4	1	−2	1	1	−1	−1	(A)
1	−1	2	0	−1	−2	1	4	0	−1	1	∞	(B1)
1	2	−1	−1	0	1	1	1	−1	0	∞	1	(B0)
1	−1	−1	0	−1	−2	1	1	0	0	1	∞	(L)
1	−1	−1	−1	0	1	1	1	0	0	∞	1	(C)

TABLE II

$(q, x, y) = (3, j^2, j)$

T	T'	T''	T_C	T_L	f	f'	f''	$d-d'$	$d-d''$	X	Y	Case
1	$-j^2$	$-j$	-1	-1	j^2-j	1	$j-j^2$	0	0	j^2	j	(B2)
1	$\frac{1-j}{3}$	$\frac{1-j^2}{3}$	$\frac{j-1}{3}$	$\frac{j^2-1}{3}$	3	1	j^2-j	1	1	j	j^2	(A)
1	j^2	$1-j^2$	0	j^2	$j-j^2$	1	3	0	-1	1	∞	(B1)
1	$1-j$	j	j	0	1	1	1	-1	0	∞	1	(B0)
1	j^2	j^2	0	j^2	$j-j^2$	1	1	0	0	1	∞	(L)
1	j	j	j	0	1	1	1	0	0	∞	1	(C)

easily seen that $f = f' + (q-1)\hat{f}$. Let α be as in Theorem 3.4. The following lemma strongly uses properties of the three values of (q, z) considered here.

6.4. LEMMA. *Suppose that the vector $u \in F^S$ is such that $\langle u, \alpha(v)\rangle = 0$ for every $v \in V'$ and that $V = V' + (u)$. Then $z^{w(u+v)} = z^{w(u)} z^{w(v)}$. It follows that $\hat{f} = z^{w(u)} f'$ and hence $f = [1 + (q-1)\, z^{w(u)}]\, f'$.*

Proof. For $q = 2, 3, 4$ let r be, respectively, 4, 3, 2, so that $z^r = 1$ in each case. In each case it is readily verified that if $\langle u, \alpha(v)\rangle = 0$, then $w(u+v) \equiv w(u) + w(v) \pmod{r}$. The conclusions follow. ∎

We now define the cases for each table. Throughout, S is a finite set, V is an $\mathbb{F}_q$-space on S and $s \in S$.

For Table I, let $q = 4, z = -1, (x, y) = (-1, -1)$. Let α be such that $\alpha(a) = a^{-1}$ for all $a \neq 0$. Let cases (L) and (C) hold when s is a loop or

TABLE III

$(q, x, y) = (2, -i, i)$

T	T'	T''	T_C	T_L	f	f'	f''	$d-d'$	$d-d''$	X	Y	Case
0	1	-1	i	i	0	1	$1+i$	1	1	$-i$	i	(A.2)
1	$\frac{1-i}{2}$	$\frac{1+i}{2}$	$\frac{-1+i}{2}$	$\frac{-1-i}{2}$	2	1	$1-i$	1	1	i	$-i$	(A.0)
1	0	1	-1	$-1-i$	i	0	1	-1	0	0	-1	(B03)
1	1	0	$-1+i$	-1	$1-i$	1	0	0	-1	-1	0	(B13)
1	$-i$	$1+i$	0	$-i$	$1+i$	1	2	0	-1	1	∞	(B11)
1	$1-i$	i	i	0	1	1	1	-1	0	∞	1	(B01)
1	$-i$	$-i$	0	$-i$	$1+i$	1	1	0	0	1	∞	(L)
1	i	i	i	0	1	1	1	0	0	∞	1	(C)
0	0	0	0	0	0	0	0					(..2)

coloop, respectively, and let cases (A), (B0), (B1) hold when s is not a loop or coloop, but is of type (A), (B0), (B1), respectively. Note that s is never of type (Ba) where $a \in \mathbb{F}_4 - \{0, 1\}$; since otherwise there would exist $v \in V, u \in \alpha(V^*)$ such that $v(s) = a$ and $v + u = 1_s$, so that $\mathrm{supp}(v) = \mathrm{supp}(u)$ and $\mathbb{F}_4 \ni 0 = \langle u, \alpha(v) \rangle = w(v) - 1 + (1 - a)\,\alpha(a) = w(v) + a^{-1} \neq 0$; a contradiction.

For Table II, let $q = 3$, $z = j$, $(x, y) = (j^2, j)$. Let cases (L) and (C) hold when s is a loop or coloop, respectively, and let cases (A), (B0), (B1), (B2) hold when s is not a loop or coloop, but is of type (A), (B0), (B1), (B2), respectively.

For Table III, let $q = 2$, $z = i$, $(x, y) = (-i, i)$. Let case (..2) hold when there exists $v \in V \cap V^*$ with $v(s) = 0$ and $w(v) \equiv 2 \pmod 4$. Let cases (L) and (C) hold when (..2) does not hold and s is a loop or coloop, respectively. Let cases (A.m), $m = 0, 2$, hold when (L), (C), (..2) do not hold, s is of type (A) and there exists $v \in V \cap V^*$ with $v(s) = 1$ and $w(v) \equiv m \pmod 4$. (It is clear that $w(v)$ must be even.) Let cases (B1m), $m = 1, 3$, hold when (L), (C), (..2) do not hold, s is of type (B1) and there exists $v \in V$ with $v(s) = 1$ and $v + 1_s \in V^*$ and $w(v) \equiv m \pmod 4$. (It is clear that $w(v)$ must be odd.) Let cases (B0m), $m = 1, 3$, hold when (L), (C), (..2) do not hold, s is of type (B0) and there exists $v \in V^*$ with $v(s) = 1$ and $v + 1_s \in V$ and $w(v) \equiv m \pmod 4$. (Again, $w(v)$ clearly must be odd.) Considering Lemma 6.2, it is clear that at least one case must hold and the only possibility of more than one holding is if both (A.0) and (A.2) hold or both (B11) and (B13) hold or both (B01) and (B03) hold. But it is routine to check that if any of these pairs held, then so would (..2), a possibility excluded by the definitions, so that exactly one of the cases in Table III holds.

The entries for $d - d'$ and $d - d''$ are left blank for case (..2) since they depend on whether s is of type (A), (B1) or (B0). However, it will be shown that $T = 0$ in this case, so that in proving Theorem 3.4 and Lemma 6.1, the value of d does not matter.

6.5. Lemma. *In each of the three tables and for every V and s, exactly one case holds, that case can be determined in polynomial time, and the entries in the table are correct.*

Proof. The above discussions justify that exactly one case holds. In polynomial time, we can determine the *type* of s, by Lemma 6.2; whether s is a loop or coloop; the weight of the vector v in Lemma 6.2; and, in the $q = 2$ case, whether or not (..2) holds.

The correctness of the entries in the $d - d'$ and $d - d''$ columns follow from Lemma 6.3.

By Equations (12)–(14) and (22), the ratio between any two of T, T', T'', T_C, T_L or any two of f, f', f'' determines all other such ratios as well as (X, Y). It is routine to check that all the rows are consistent. Thus we need to show that, in each row, one such ratio is correct.

If s is of type (A) or (Ba) with $a \neq 0$, then considering Lemma 6.2 we can find a vector u satisfying the hypotheses of Lemma 6.4, and giving the required ratio $f : f'$. (This u is actually the v given by Lemma 6.2.) If s is of type (B0) with respect to V, then it is of type (B1) with respect to V^*. Using Equation (15) we can deduce the (B0) case from the (B1) case.

The argument for case (A.2) shows that if there exists $v \in V \cap V^*$ with $w(v) \equiv 2 \pmod 4$, then $T = 0$. In case (..2) there is such a v with $v(s) = 0$ so that $v - s \in V \backslash s \cap V^*/s = V \backslash s \cap (V \backslash s)^*$ and $w(v - s) = w(v)$ and hence $T = T' = 0$, as required. ∎

Proof of Lemma 6.1. Suppose the input matroid M is represented by F-space V, which in turn is represented by a basis of V. Choose $s \in S$, determine which case applies to (M, s) and hence find the ratio $T : T'$ or $T : T''$. (If T' and T'' are both zero, then so is T and the answer is already found.) Repeat the process with T' (or T'' if $T' = 0$) and proceed inductively until after $|S|$ such steps, the empty matroid (whose Tutte polynomial is 1) is reached. Multiplying the $|S|$ ratios gives T, computed in polynomial time, as required. ∎

7. PROOFS

The proofs of the main theorems are virtually complete.

Proof of Theorem 3.1. As shown in [18], all the Tutte invariants are in $\overline{\#\mathrm{P}}$. Since $\mathscr{G} \subseteq \mathscr{M}_F$ (for any F) it follows from Proposition 2.2 and Lemma 2.1 that we need only consider the special points other than (0, 0) (which is in H_1).

In [17], it is shown that $\tau^0(\mathscr{M}_F, 1, 1)$ is $\overline{\#\mathrm{P}}$-complete for every field F. As noted in [11], for binary space V with $M(V) = (S, \rho)$, $T(M(V), -1, 0)$ is 0 if V (and hence every basis for V) has an element of odd weight, and is $(-1)^{|S| - \rho(S)}$ otherwise. So $\tau^0(\mathscr{M}_2, -1, 0)$ and similarly $\tau^0(\mathscr{M}_2, 0, -1)$ is in FP. Also $T(M; i, -i)$ and $T(M; j, j^2)$ are, respectively, the complex conjugates of $T(M; -i, i)$ and $T(M; j^2, j)$. The remaining cases follow from Lemmas 5.1 and 6.1. ∎

Proof of Theorem 3.4. This follows from the material in Section 6. ∎

8. FURTHER CONCLUSIONS

By combining Lemmas 5.2 and 5.3 with some excluded minor results, we can obtain a more complete answer to complexity questions about Tutte invariants for various classes of matroids.

3. DEFINITION. The class of matroids $\mathscr{C}$ (together with encoding e: $\{0,1\}^* \to \mathscr{C}$) is 2-*sum-succinct* if:

(i) $\mathscr{C}$ (together with encoding e) is *expand-succinct*, and

(ii) the class of matroids $\mathscr{C}$ is closed under 2-sums and minors and these can be constructed in polynomial time.

Note that $\mathscr{G}$, $\mathscr{M}_{\text{reg}}$ and $\mathscr{M}_F$ are all 2-sum-succinct for every finite field F.

We use the following excluded minor results due to [14], [1], [13], [7]. All of the matroids below are defined in [12] except P_8'' (see also [7]) which is obtained from P_8 by relaxing the unique pair of disjoint circuit-hyperplanes.

8.1. THEOREM. *The sets of excluded minors of* $\mathscr{M}_2$, $\mathscr{M}_3$, *and* $\mathscr{M}_4$ *are* $\{U_{2,4}\}$, $\{U_{2,5}, U_{3,5}, F_7, F_7^*\}$, *and* $\{U_{2,6}, U_{4,6}, P_6, F_7^-, (F_7^-)^*, P_8, P_8''\}$, *respectively.*

Let $\hat{\mathscr{M}}_4$ be the class of matroids which are direct-sums and 2-sums of quaternary matroids, P_8'' and minors of the matroid $S(5,6,12)$ (see [12]). Note that there are only ten 3-connected non-quaternary matroids in $\hat{\mathscr{M}}_4$. The following is proved in [8].

8.2. THEOREM. *The set of excluded minors of* $\hat{\mathscr{M}}_4$ *is* $\{U_{2,6}, U_{4,6}, P_6, F_7^-, (F_7^-)^*\}$.

For $q \in \{2,3\}$, let $\hat{\mathscr{M}}_q = \mathscr{M}_q$. We can characterise exactly which closed classes contain spoilers for which movable special points.

8.3. THEOREM. *Let* (x, y) *be a movable special point with* $q = (x-1)(y-1)$. *Let* $\mathscr{C}$ *be a 2-sum-succint class of matroids. Then* $\mathscr{C}$ *contains a spoiler for* (x, y) *if and only if* $\mathscr{C} \not\subseteq \hat{\mathscr{M}}_q$.

Proof. Combining Lemma 5.3, Theorem 8.1 and Theorem 8.2, we need only show that $(-1,-1)$ has no spoiler in $\hat{\mathscr{M}}_4 - \mathscr{M}_4$. It is routine to check the ten 3-connected matroids in $\hat{\mathscr{M}}_4 - \mathscr{M}_4$ and the other matroids in $\hat{\mathscr{M}}_4 - \mathscr{M}_4$ can be dealt with by an inductive argument. ∎

This gives rise to the following computational complexity result.

8.4. THEOREM. *Let $\mathscr{C}$ be a 2-sum-succinct class of matroids. Let (x, y) be a movable special point with $q=(x-1)(y-1)$ so that $(x, y)\in H_q$ with $q\in\{2, 3, 4\}$. Let $\mathscr{C}$ be a closed class of matroids.*

(i) *If $\mathscr{C}\subseteq\hat{\mathscr{M}}_q$, then $\tau^0(\mathscr{C}, x, y)$ is in* FP.

(ii) *If $\mathscr{C}\not\subseteq\hat{\mathscr{M}}_q$, then $\tau^1(\mathscr{C}, H_q)\leqslant_T\tau^0(\mathscr{C}, x, y)$.*

(iii) *If $\mathscr{G}\subseteq\mathscr{C}$, but $\mathscr{C}\not\subseteq\hat{\mathscr{M}}_q$, then $\tau^0(\mathscr{C}, x, y)$ is $\overline{\#\mathrm{P}}$-complete.*

Proof. Part (i) follows from Lemma 6.1 except in the case that $(q, x, y)=(4, -1, -1)$. Extending the algorithm from $\mathscr{M}_4$ to $\hat{\mathscr{M}}_4$ is routine, but we omit the tedious details.

Part (ii) follows from Lemma 5.2 and Theorem 8.3. Part (iii) follows from Proposition 2.2 and (ii). ▮

It can be shown that the polynomial-time computability results in Theorem 8.4(i) hold even if the input is in the form of a rank-oracle, using results in [6], [4].

We finally consider the complexity of Tutte invariants when the input class is $\mathscr{M}_F$ for some infinite field F. An apparent problem is that there may not be a rank-succinct encoding for $\mathscr{M}_F$ and we cannot assume that there is one. (This is an open question even for $F=\mathbb{Q}$.) However, recall Equation (3) and its hypotheses on classes of matroids $\mathscr{C}'$ and $\mathscr{C}$ with $\mathscr{C}=\mathscr{M}_F$. To show that some Tutte invariant with input class $\mathscr{C}$ is $\overline{\#\mathrm{P}}$-complete it is sufficient to show that it is $\overline{\#\mathrm{P}}$-complete when restricted to a class $\mathscr{C}'$ satisfying the hypotheses of Equation (3). For non-special points not on H_1 we may use $\mathscr{C}'=\mathscr{G}$. For movable special points we may let $\mathscr{C}'$ be the class of tensor products of graphs with an appropriate spoiler from Lemma 5.3. In either case a matrix representation of a matroid in $\mathscr{C}$ can be constructed in polynomial time, (with the matrix having a bounded number of entries). Thus we may state the following theorem which covers the infinite field case.

8.5. THEOREM. *Let F be a field with $|F|\geqslant 5$. Suppose $\mathscr{M}_F$ is encoded so that for any matroid $M\in\mathscr{M}_F$, the size and rank of M can be found in polynomial time. (The encodinq need not be rank-succinct.) Then for any algebraic curve K and any algebraic point (x, y), the Tutte invariants $\tau^2(\mathscr{M}_F)$, $\tau^1(\mathscr{M}_F, K)$ and $\tau^0(\mathscr{M}_F, x, y)$ are all $\overline{\#\mathrm{P}}$-complete, except for $\tau^1(\mathscr{M}_F, H_1)$ and $\tau^0(\mathscr{M}_F, x, y)$ with $(x, y)\in H_1$ which are in* FP.

Proof. The $\overline{\#\mathrm{P}}$-completeness of $\tau^0(\mathscr{M}_F, 1, 1)$ is shown in [17]. The rest follows from Lemma 2.1, Proposition 2.2, Lemma 5.2, Lemma 5.3, and the comments above. ▮

REFERENCES

1. R. E. Bixby, On Reid's characterization of the ternary matroids, *J. Combin. Theory Ser. B* **26** (1979), 174–204.
2. T. H. Brylawski, A decomposition for combinatorial geometries, *Trans. Amer. Math. Soc.* **171** (1972), 235–282.
3. T. H. Brylawski, The Tutte polynomial, *in* "Matroid Theory and Its Applications," Vol. 3, pp. 125–275, Centro Internazionale Matematico Estivo, 1980.
4. C. R. Coullard, J. G. Oxley, and D. L. Vertigan, A polynomial time algoritm for constructing a representation of a quaternary matroid from a rank oracle, in preparation.
5. H. Crapo, The Tutte polynomial, *Aequationes Math.* **3** (1969), 211–229.
6. W. H. Cunningham, "A Combinatorial Decomposition Theory," Ph.D. Thesis, University of Waterloo, 1973.
7. J. F. Geelen, A. M. H. Gerards, and A. Kapoor, The excluded minors for GF(4)-representable matroids, submitted for publication.
8. J. F. Geelen, J. G. Oxley, D. L. Vertigan, and G. P. Whittle, On the excluded minors for quaternary matroids, submitted for publication.
9. C. Greene, Weight enumeration and the geometry of linear codes, *Stud. Appl. Math.* **55** (1976), 119–128.
10. F. Jaeger, Tutte polynomials and bicycle dimension of ternary matroids, *Proc. Amer. Math. Soc.* **107** (1989), 17–25.
11. F. Jaeger, D. L. Vertigan, and D. J. A. Welsh, On the computational complexity of the Jones and Tutte polynomials, *Math. Proc. Cambridge Philos. Soc.* **108** (1990), 35–53.
12. J. G. Oxley, "Matroid Theory," Oxford Univ. Press, New York, 1992.
13. P. D. Seymour, Matroid representation over GF(3), *J. Combin. Theory*, *Ser. B* **26** (1979), 159–173.
14. W. T. Tutte, A homotopy theorem for matroids, I, II, *Trans. Amer. Math. Soc.* **88** (1958), 144–174.
15. W. T. Tutte, A ring in graph theory, *Proc. Cambridge Philos. Soc.* **43** (1947), 26–40.
16. L. G. Valiant, The complexity of enumeration and reliability problems, *SIAM. J. Comput.* **8** (1979), 410–421.
17. D. Vertigan, Counting bases in matroids, unpublished manuscript.
18. D. Vertigan, "On the Computational Complexity of Tutte, Jones, Homfly and Kauffman Invariants," D.Phil. Thesis, University of Oxford, 1991.
19. D. J. A. Welsh, "Complexity: Knots, Colourings and Counting," London Mathematical Society Lecture Note Series 186, Cambridge Univ. Press, Cambridge, UK, 1993.
20. H. Whitney, A logical expansion in mathematics, *Bull. Amer. Math.* **57** (1935), 509–533.